REMARKS

The above-referenced patent application has been reviewed in light of the Office Action referenced above. Reconsideration of the above-referenced patent application in view of the following remarks is respectfully requested.

Claims 156 and 158-181 are pending in the application. Claims 156, 159, 160, 162, 165, 166, 168-170, 172, 173, 175, 178, 179, and 181 have been amended. Claims 182-191 have been added. The amendment is fully supported by the original disclosure. No new matter has been introduced. Assignee asserts that no prosecution history estoppel should result from the above amendments where the amendments were made to clarify Assignee's claims and/or broaden scope of the amended claims.

Claim rejections - 35 USC §103

Claims 156-179 are rejected under 35 U.S.C. 103(a) over Shear (US Pat. No. 4,827,508) in view of Matyas, Jr. et al. (US Pat. No. 4,850,017) and further in view of Sklut et al. (US Pat. No. 5,270,773). Claims 180-181 are rejected under 35 U.S.C. 103(a) over Shear and Matyas and Sklut as applied to claims 156-179 above, and further in view of Atalla (US Pat. No. 4,588,991). Assignee respectfully disagrees with these rejections; however, Assignee has amended claims to further prosecution.

Assignee respectfully submits the Examiner has not established that the proposed combination discloses all of the elements of independent claim 156. The Examiner is kindly reminded that the Examiner's initial burden of factually supporting any *prima facie* conclusion of obviousness includes that:

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. MPEP § 2143.03.

For example, Examiner has not established that the proposed combination discloses a "*permit key capable of use in cryptographic operations and pre-defined to permit at least one use of digital data comprising one or more of the following functions of: displaying, editing, storing, copying, or transferring, or combinations thereof*", as recited in claim 156. In the present Office Action, the Examiner concedes that Shear does not disclose such a feature:

> Shear does not disclose the keys corresponding to at least one of different types of uses of digital data requested by the user, each of the utilization permit keys permitting only the corresponding at least one of the different types of uses of the digital data. (See page 3 of the Office Action)

The Examiner attempts to cure Shear of this failure through combination with Matyas, asserting:

> Matyas discloses a method and system for controlling the use of a cryptographic key at a using station by a generating station in a network of generating and using stations (abstract). The system of Matyas discloses supplying to a user at least one of a plurality of utilization permit keys that correspond only to at least one of different types of uses of digital data requested by the user (column 8 lines 7-61) . (See page 4 of the Office Action)

The Examiner also attempts to cure Shear of this failure through combination with Sklut, asserting:

> Sklut discloses a system wherein depending on the operator's access level, i.e. authority to view sensitive documents, the image producing device enables a purge or the existing sensitive documents or electronic images or prevents operation until an authorized operator initiates a purge (abstract). Therefore Shear

> discloses utilizing permit keys (column 4 lines 10-12 that permit the different uses of digital data including printing and copying (column 2 lines 25-44). (See page 4 of the Office Action)

Assignee respectfully disagrees, Specifically, the Examiner has not established that the predefined access algorithm of Shear has anything to do with a "*permit key capable of*" **both** "*use in cryptographic operations*" and "*pre-defined to permit at least one use of digital data comprising one or more of the following functions of: displaying, editing, storing, copying, or transferring, or combinations thereof*", as claimed. Neither the "access algorithm" nor the "multiple levels of security codes" of Shear appear related to the "decryption key" described in Shear. For example, column 11, line 64 to column 12, line 2 of Shear discusses the predefined access algorithm of Shear as operating without encryption as follows:

> In one possible permutation of the invention, neither the database nor the index stored on medium 100 is "encrypted" using a formal encryption algorithm, but instead, the manner in which the database and/or the index is stored on the storage medium is itself used to make information incoherent unless it is read from the medium using a predefined access algorithm. (See column 11, line 64 to column 12 line 2 of Shear)

Accordingly, the predefined access algorithm of Shear appears to teach away from use of a "*permit key*" capable of "*use in cryptographic operations*" in addition to being capable of "*pre-defined to permit at least one use of digital data*", as recited in claim 156. Likewise, the "multiple levels of security codes" of Shear do not appear related to the "decryption key" described in Shear. For example, the "identification and/or password information" of Shear appears to be supplied by a user to confirm authorization of a user at step 410 of Figure 4, whereas the "predetermined conventional decryption algorithm" of Shear appears to be stored in logic 310 to decrypt data at step 418 of Figure 4. See column 15, lines 3-21 and column 16,

lines 42-56 of Shear. Accordingly, the "identification and/or password information" of Shear of Shear appears to teach away from use of a "*permit key*" capable of **both** "*use in cryptographic operations*" and "*pre-defined to permit at least one use of digital data*", as recited in claim 156.

Further, Assignee can find no support in column 7 lines 57-67 or in column 8 lines 7-61 of Matyas for a plurality of crypt keys corresponding to "*pre-defined to permit at least one use of digital data*", as recited in claim 156. Rather, the Examiner has only cited to portions of Matyas prescribing how the crypt key itself may be limited to one use or another, but the Examiner has not established that any portion of Matyas discusses any limitation on the "*use of digital data*", as recited in claim 156. Specifically, the Examiner has not established that the Key Usage Function (KUF) based on control value C of Matyas is directly relevant to any limitation on the "*use of digital data*", as recited in claim 156. Conversely, column 7, line 57 to column 8 line 6 of Matyas discusses the control value C as follows:

> The cryptographic facility at each station in the network configuration of FIG. 1 has a Key Generation Function (KGF) and a Key Usage Function (KUF). Each key generated by a KGF has an associated control value C which prescribes how the key may be used; e.g., encrypt only, decrypt only, generation of message authentication codes, verification of message authentication codes, etc. The KUF provides a key authorization function to ensure that a requested usage of a key complies with the control value C, and in one aspect of the described invention it also serves as an authentication function to ensure that a requested key and control value are valid before allowing the key to be used. Thus, the KUF is the logical component of the cryptographic facility that enforces how keys are used at each using station, and in this sense, the KUFs collectively enforce the overall network key usage as dictated by the generating station. (See column 7, line 57 to column 8 line 6 of Matyas)

Here, Assignee submits that the Examiner has failed to establish that the prescription of the control value C of Matyas for "encrypt only, decrypt only, generation of message authentication codes, verification of message authentication codes" teaches or suggests any restriction on the "*use of digital data*", let alone restriction on the recited uses of "*pre-defined to permit at least one use of digital data comprising one or more of the following functions of: displaying, editing, storing, copying, or transferring, or combinations thereof*", as recited in claim 156.

Further, Assignee can find no support in Sklut for a "*permit key*" **both** "*use in cryptographic operations*" and "*pre-defined to permit at least one use of digital data*", as recited in claim 156. Rather, the Examiner has only cited to portions of Sklut prescribing how a key of the "some form of operator password login system 11" of Sklut may limit access rights, but the Examiner has not established that any portion of Sklut discusses "*use in cryptographic operations*", as recited in claim 156. Specifically, the Examiner has not established that the key of the "some form of operator password login system 11" of Sklut is directly relevant to "*use in cryptographic operations*", as recited in claim 156. Conversely, Assignee can find no reference in Sklut regarding encryption, decryption, or cryptography in general.

Elsewhere in the Office Action, the Examiner has asserted that different uses are disclosed in Shear:

As per claim 157, the limitations of the different uses of digital data including